De werking van de WBP in kaart gebracht

Winter, H.B.

Published in:
RegelMaat

Publication date:
2009

De werking van de WBP in kaart gebracht: onbekend maakt onbemind

H.B. Winter

1. Inleiding

De Wet bescherming persoonsgegevens (WBP) trad op 1 september 2001 in werking.[1] De wet is de 'opvolger' van de Wet persoonsregistraties (WPR) en is tot stand gekomen ter implementatie van de Europese Privacyrichtlijn.[2] Het doel van de wet is het bieden van waarborgen ter realisatie van een evenwicht tussen privacybescherming en andere belangen. Daarnaast wenst de wetgever de positie van personen van wie gegevens worden verwerkt, te versterken door aan hen een aantal rechten (zoals het inzage- en het correctierecht) toe te kennen. In dat verband legt de wet aan de verantwoordelijke (degene die zeggenschap heeft over het doel en de wijze van verwerking van persoonsgegevens) plichten op, zoals de meldings- en informatieplicht. Het College bescherming persoonsgegevens (CBP) is aangewezen als onafhankelijk toezichthouder. Organisaties kunnen een Functionaris Gegevensbescherming (FG) aanstellen, die intern toezicht houdt op de naleving van de wet.

Persoonsgegevens kunnen worden verwerkt na een zorgvuldige afweging van de belangen van de verantwoordelijke en de belanghebbende. Deze belangenafweging is voorgeschreven in artikel 8 onder f WBP: is de verwerking noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke en is de verwerking evenredig in verhouding tot het belang van de betrokkene? De wet kent geen sluitend stelsel van concrete materiële normen over wat wel en niet is toegestaan. In concrete situaties waarin persoonsgegevens worden verwerkt, moet dus telkens weer die afweging worden gemaakt. Een uitzondering geldt voor bijzondere persoonsgegevens. Deze gegevens mogen alleen worden verwerkt als de wet dat toestaat. De wetgever geeft in de toelichting aan dat de bepaling inzake de afweging van belangen een kameleontisch karakter heeft. Of een aanvaardbare afweging heeft plaatsgevonden, is afhankelijk van de context waarin de gegevensverwerking plaatsvindt. Bij gegevensverwerking in de publieke sector wordt getoetst of de afweging voldoet aan de bestuursrechtelijke beginselen van behoorlijk bestuur. Bij de private sector wordt getoetst of is voldaan aan de zorgvuldigheid die volgens het ongeschreven recht in het maatschappelijk verkeer betaamt.

In het evaluatieonderzoek is de werking van de wet in kaart gebracht.[3] In deze bijdrage worden de belangrijkste uitkomsten van dat onderzoek beschreven. Nadat ik

1 *Stb.* 2000, 302.
2 Richtlijn 95/46/EG, *PbEG* L 281.
3 H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg & H. Prakken, *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Den Haag: Boom Juridische uitgevers 2009.

in paragraaf 2 de opzet en uitvoering van het onderzoek kort belicht heb, ga ik in paragraaf 3 in op de open normen van de wet en de gevolgen die dat voor de privacypraktijk heeft. In paragraaf 4 komen de informatie- en meldingsplichten uit de wet aan de orde. Tevens wordt daarbij aandacht besteed aan de mate waarin betrokkenen gebruikmaken van hun rechten. Paragraaf 5 gaat in op toezicht en rechtsbescherming. Een afsluitende conclusie over de werking van de wet wordt gepresenteerd in paragraaf 6.

2. Opzet en uitvoering

De probleemstelling van het onderzoek luidde als volgt*: In hoeverre voldoet de werking van de WBP in de praktijk aan de doelstellingen van de wet, in het bijzonder gelet op de in de literatuur gesignaleerde knelpunten, en welke aanpassingen zijn mogelijk en wenselijk binnen het kader van de EU-richtlijn?* Om die onderzoeksvraag te beantwoorden is begonnen met literatuuronderzoek. Vervolgens is een oriënterende interviewronde gehouden. Het kwantitatieve deel van het onderzoek bestond uit schriftelijke enquêtes. Allereerst is er een *algemene enquête* verzonden naar 638 organisaties, geselecteerd uit een lijst van bestuursorganen en uit het handelsregister van de Kamer van Koophandel. Dertien procent van de aangeschreven organisaties heeft gereageerd. De steekproef was gestratificeerd, er is gezocht naar organisaties die naar verwachting vaak persoonsgegevens verwerken. Vervolgens is een steekproef getrokken uit het meldingenbestand bij het CBP. Naar 647 bedrijven, instellingen en overheden die bij het CBP een melding hebben gedaan van het verwerken van persoonsgegevens, is een *meldingenenquête* verstuurd. Hiervan heeft 26 procent gereageerd. Ten slotte zijn alle 215 bij het CBP aangemelde interne toezichthouders, de functionarissen voor de gegevensbescherming (FG's) als bedoeld in artikel 62 WBP, aangeschreven. Van hen heeft 34 procent op de *FG-enquête* gereageerd. Ook is gesproken met burgers. Hiervoor zijn niet willekeurige burgers benaderd, maar burgers die een geschil over de WBP aanhangig hebben gemaakt. Dit onderzoek is langs telefonische weg uitgevoerd.

Behalve dit kwantitatieve onderzoek is ook meer kwalitatief onderzoek uitgevoerd. Hiervoor zijn twee casestudyonderzoeken verricht bij samenwerkingsverbanden. Eén samenwerkingsverband is een veiligheidshuis, waarin politie, justitie en hulpverleningsinstanties met elkaar samenwerken. Het andere samenwerkingsverband betreft een instelling voor de geestelijke gezondheidszorg, waarin verslavingszorg en GGZ samenwerken. Voor deze casus is gekozen vanwege het grote aantal organisaties dat in die gevallen met elkaar samenwerkt, en de uit het oogpunt van het belang van privacy kwetsbare situaties die daarbij aan de orde zijn.

Na deze onderzoeken zijn verdiepende interviews en enkele expertmeetings (met intermediaire burgerorganisaties, juridisch experts en FG's) georganiseerd.

Tabel 1: Duidelijkheid van de wettelijke norm over verwerking persoonsgegevens

	Het is ons altijd volledig duidelijk welke persoonsgegevens we mogen verwerken		
	Organisaties in steekproef handelsregister (%)	Meldende organisaties (%)	Organisaties met een FG (%)
Zeer mee eens	40,5	5,7	7,3
Mee eens	35,4	40,3	37,7
Neutraal	20,3	31,4	18,8
Mee oneens	3,8	18,2	33,3
Zeer mee oneens	0,0	4,4	2,9
Totaal	100	100	100

3. Open normen

Er is een breed draagvlak voor de keuze van de wetgever voor open normen als wetgevingstechniek. De professionals die met de wet werken, noemen als voordelen de mogelijkheid de normen nader in te vullen per branche of in een bepaalde context, de mogelijkheid rekening te houden met onvoorziene omstandigheden, en de geschiktheid van open normen gelet op het belang van technologische ontwikkelingen voor privacybescherming. Niettegenstaande dat draagvlak en de gepercipieerde voordelen moet tegelijkertijd worden vastgesteld dat nadere normstelling nog niet overal tot ontwikkeling is gekomen. Volgens het enquêteonderzoek zijn sectorale normen in iets meer dan de helft van de sectoren ontstaan. Organisaties hebben kennelijk nog wel een duwtje nodig. Hoewel het CBP op dat vlak wel het een en ander doet, zoals het uitgeven van informatiebladen, het publiceren van richtsnoeren en het bemiddelen in concrete geschillen, is nog niet bij alle ondervraagde verantwoordelijken sprake van voldoende duidelijkheid over de invulling van de open normen. De activiteiten van het CBP worden niet gezien als een sterke stimulans in die richting. Dat nadere normstelling nog niet overal tot ontwikkeling is gekomen, is wel verrassend gelet op de administratieve lasten die invulling van de open normen in concrete situaties met zich meebrengt. Het onderzoek laat zien dat juist die lasten sterk bepalend zijn voor de tevredenheid over de wet.

Een merkwaardige paradox in de onderzoeksresultaten is dat daaruit afgeleid kan worden dat hoe minder organisaties met de wet te maken hebben, des te meer ze zeggen duidelijkheid te hebben over de vraag of persoonsgegevens mogen worden verwerkt. Anders gezegd: naarmate organisaties meer met de wet werken, neemt ook het aantal problemen in de uitvoeringspraktijk toe. 'Wat niet weet, wat niet deert' is daarmee een rode draad in de onderzoeksbevindingen.

Tabel 2: Informatieplicht betrokkenen

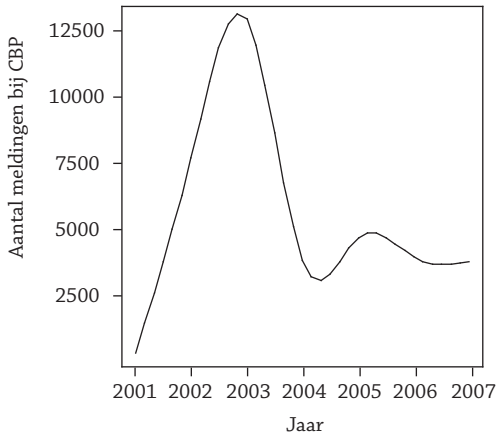
Informatie over verwerkingen	Organisaties in steekproef handelsregister (%)	Meldende organisaties (%)	Organisaties met een FG (%)
Op de website	26	33	51
Op aanvraagformulieren	51	27	35
In folders	24	24	25
Algemene voorwaarden	38	28	23
Persoonlijk schrijven	29	26	16
Anders	13	39	20

Die bevinding is niet alleen gerapporteerd op basis van de enquêtes. Ook de casestudies van een 'veiligheidshuis' en een 'inrichting voor opvang van verslaafde daken thuislozen' leiden tot dezelfde conclusie. Men komt vaak niet eens toe aan de vraag hoe de normen van de wet moeten worden geïnterpreteerd. Onbekendheid van de norm en geringe bereidheid in deskundigheidsbevordering te investeren blijken in de praktijk grotere problemen. Dat de wet een knelpunt zou opleveren voor ketensamenwerking, is dan ook niet per se het gevolg van de wet, maar veeleer een gevolg van het feit dat in samenwerkingsverbanden het beleidsdoel dat met de samenwerking wordt beoogd, centraal staat. Privacybescherming delft daarbij vaak het onderspit.

4. Informatie- en meldingsplichten en rechten van betrokkenen

Een burger heeft diverse rechten die door de WBP worden gewaarborgd. Om te beginnen moet een burger worden geïnformeerd dat persoonsgegevens worden verwerkt. Verder heeft hij het recht op inzage en kan hij verzoeken om correctie of aanvulling van de gegevens. Wanneer gebruikmaking van die rechten niet leidt tot het gewenste resultaat, kan een burger een geschil aanhangig maken. Daarvoor zijn verschillende wegen te bewandelen: het indienen van een klacht bij de Nationale ombudsman, de weg naar de civiele rechter, de bestuursrechter (al dan niet voorafgegaan door bezwaar) of een geschillencommissie. Ook kan een verzoek om bemiddeling worden voorgelegd aan het CBP. Over de informatieplicht rapporteren de geënquêteerde organisaties dat deze taak ertoe heeft geleid dat hun organisatie zorgvuldiger omgaat met persoonsgegevens en privacy. Dat leidt er volgens de onderzoeksgegevens toe dat driekwart van de organisaties de betrokkene informeert over de verwerking van zijn persoonsgegevens. Daarvoor worden verschillende methoden gehanteerd.

Figuur 1: Kwantitatieve ontwikkeling van het CBP-meldingenregister



Hoewel betrokkenen dus redelijk goed lijken te worden geïnformeerd over het gebruik van de mogelijkheden die de WBP biedt om inzage te krijgen in de over hen verzamelde gegevens, geeft slechts een op de drie organisaties aan wel eens met zo'n verzoek om inzage te worden geconfronteerd. Verzoeken om correctie en aanvulling komen iets vaker voor (bij een op de vijf regelmatig, bij de helft soms, bij een op de vijf nooit). Een opvallende bevinding is dat hoewel betrokkenen dus niet vaak gebruik lijken te maken van hun recht tot inzage, correctie of aanvulling, organisaties toch nog redelijk vaak (ruim een op de drie) een procedure hebben vastgesteld voor de wijze waarop ze op dergelijke verzoeken moeten reageren.

Uit diverse bronnen blijkt dat burgers een veel groter vertrouwen hebben in overheden dan in bedrijven als het gaat om de wijze waarop organisaties met hun persoonsgegevens omgaan. Geraadpleegde experts zijn over het algemeen kritischer over de wijze waarop overheden met persoonsgegevens omgaan. Bedrijven hebben vaak een kwetsbare klantrelatie, die kan worden verbroken bij ontevredenheid over de verwerking van persoonsgegevens. Daarbij is van belang dat klanten naar de concurrent kunnen gaan. Die mogelijkheid hebben burgers bij de overheid vaak niet. Het behoud van het vertrouwen van de klant is dan ook de belangrijkste reden voor bedrijven bij het doen van een melding bij het CBP.

Artikel 27 WBP bepaalt dat verwerkingen van persoonsgegevens gemeld moeten worden bij het CBP, of, indien de organisatie over een FG beschikt, bij deze FG. Een groot aantal veelvoorkomende verwerkingen is opgenomen in het Vrijstellingsbesluit, en is daarom op grond van artikel 28 WBP vrijgesteld van de meldingsplicht. De meldingsplicht lijkt redelijk te worden nageleefd. Het merendeel van de organisaties kent de verplichting en zegt zich eraan te houden. Een beperkt deel van de organisaties in de steekproef geeft aan de verplichting niet te kennen. Een nog kleinere groep kent de verplichting wel, maar wenst zich daaraan niet te houden. Daarbij

moet wel worden aangetekend dat het onderzoek zich richtte op de wat grotere organisaties binnen sectoren waar relatief vaak met bestanden met persoonsgegevens wordt gewerkt. Het kennisniveau binnen kleinere organisaties zou wel eens geringer kunnen zijn, waardoor niet uitgesloten kan worden dat de meldingsplicht daar minder goed wordt nageleefd. Tegelijkertijd zijn er daar waarschijnlijk minder vaak verwerkingen die gemeld moeten worden.

Interessanter is natuurlijk de vraag of de meldingsplicht een positief effect heeft op de privacy van burgers. Uit het onderzoek komt naar voren dat dit inderdaad het geval is, maar het toezicht van het CBP speelt daarbij geen enkele rol – dat toezicht op de meldingsplicht is er namelijk niet of nauwelijks (zie hierna in par. 5). Het effect zit vooral in het feit dat organisaties als gevolg van de op hen rustende meldingsplicht beter gaan nadenken over de doelen van de verwerking en daarbij een afweging maken tussen het privacybelang en het doel van de registratie, dus het belang dat de organisatie heeft bij de verwerking van de gegevens. Dát moet worden gemeld bij het CBP als zodanig, lijkt dus geen toegevoegde waarde te hebben, de melding lijkt de kennis die betrokkenen hebben van de over hen verzamelde gegevens, niet of nauwelijks te vergroten. Betrokkenen weten het meldingenregister niet te vinden; er wordt ook wel geklaagd over de toegankelijkheid daarvan.

Overigens lijken de administratieve lasten van de meldingsplicht redelijk binnen de perken te blijven. Voor zover daarover wel opmerkingen zijn gemaakt, betreffen die de complexiteit en onduidelijkheid van het meldingenprogramma of -formulier van het CBP.

Dat – zoals hiervoor is geconstateerd – van de mogelijkheid die burgers hebben tot inzage, verwijdering of correctie van hun geregistreerde persoonsgegevens, slechts beperkt gebruik wordt gemaakt, zou erop kunnen wijzen dat betrokkenen geen risico's zien die zijn verbonden aan de registratie van hun persoonsgegevens. Tegen die achtergrond lijkt het verstandig nader onderzoek te doen naar de mate waarin betrokkenen hun rechten kennen. Dat zou mogelijk tot de conclusie kunnen leiden dat de bewustwording van de privacyrisico's die betrokkenen lopen, verder moet worden versterkt. Anderzijds is het natuurlijk ook denkbaar dat uit dat onderzoek naar voren komt dat de risico's van privacyschendingen niet als erg groot aangemerkt moeten worden.

5. Toezicht en rechtsbescherming

De bevoegdheid tot het uitoefenen van toezicht op de voorschriften van de wet is toebedeeld aan het CBP en de binnen organisaties aangestelde FG's. Er zijn slechts 250 organisaties die een FG hebben aangesteld, ongeveer 0,3 promille van het totale aantal organisaties in ons land. Veel, ook grotere en internationaal opererende bedrijven, hebben ervan afgezien een FG te benoemen. De achtergrond daarvan is dat ze de meerwaarde van die functionaris niet zien. Dat ze geen FG aanwijzen, betekent echter niet dat ze het belang van privacybescherming niet zien. Vaak hebben deze bedrijven een *privacy officer*, veelal een staffunctionaris verantwoordelijk

voor risicomanagement en kwaliteitssystemen rond de bescherming van privacy in de organisatie. De bescherming van privacy wordt door bedrijven met een *privacy officer* gezien als een kwaliteitsvereiste, dat in de richting van klanten van groot belang wordt geacht. Wanneer een bedrijf op dat punt een steek laat vallen, kan dat snel leiden tot imagoschade en dus een verliespost opleveren.

Dat organisaties een *privacy officer* aanstellen in plaats van een FG, wordt in sommige gevallen ook veroorzaakt doordat het bedrijf opereert op een consumentenmarkt en onderdeel is van een holding met vestigingen in andere landen. Uit het oogpunt van uniformiteit wordt dan voor het benoemen van een *privacy officer* gekozen met dezelfde bevoegdheden en plaats binnen de organisatie, ongeacht het land waarin de bedrijfsonderdelen gevestigd zijn. Daarbij speelt ook een rol dat de functie van FG binnen het kader van de Europese richtlijn in verschillende Europese landen op een uiteenlopende wijze is vormgegeven. Mede als gevolg daarvan is de figuur van de FG in Nederland vooral te vinden bij overheden en semioverheden. Bedrijven die wel een FG benoemen, geven aan daartoe over te gaan omdat daardoor de toezichtlast vanwege het CBP vermindert, maar vooral omdat op die manier het privacybelang wordt onderstreept. Het marketingbelang, de mogelijkheid je als organisatie te onderscheiden door de zorgvuldige behandeling van persoonsgegevens, wordt ook vaak genoemd als reden om een FG aan te stellen.

In 2007 maakte het CBP een keuze om zich voortaan sterker te concentreren op toezicht en handhaving. Andere taken – die overigens ook niet bij wet aan het college zijn opgedragen – zoals het bevorderen van normontwikkeling (zie par. 3), het bevorderen van bewustwording en het volgen van technologische ontwikkelingen, krijgen vanaf dat moment minder accent. Dat is een opvallende koerswijziging. Veel respondenten die in het kader van het onderzoek zijn geraadpleegd, missen de intermediaire rol van het college bij de ontwikkeling en uitwerking van de wet. Dat geldt voor organisaties en de *privacy officers* en functionarissen gegevensbescherming die daar zijn aangesteld, maar ook voor de vertegenwoordigers van burgerbelangen. Uit het onderzoek komt naar voren dat de informatievoorziening over de wet tekortschiet, meer in het bijzonder over de keuzes die bij nadere normstelling en in concrete situaties van gegevensverwerking gemaakt moeten worden. De voorlichtende en interpreterende functie, die het CBP voorheen uitoefende, wordt gemist. Er lijken wel initiatieven, zoals van VNO/NCW, FME/CWM en ECP.nl, te ontstaan om dat 'gat' te vullen, maar die komen slechts langzaam op gang. Er is behoefte aan instanties die zich op gezaghebbende wijze op wetsinterpretatie, normuitlegging en -ontwikkeling toeleggen. Die randvoorwaarde moet worden vervuld, willen de normen uit de wet bij het publiek en bij verantwoordelijken gaan leven.

Dat het CBP zich de laatste jaren concentreert op toezicht en handhaving, is een keuze die voortvloeit uit de beperkt beschikbare mensen en middelen en die op zichzelf te begrijpen is. Tegelijkertijd valt op dat de commissie-Brouwer-Korff, die recent adviseerde over privacy en veiligheid, een pleidooi houdt voor een nieuwe

toezichtautoriteit, die zich specifiek zou moeten toeleggen op toezicht en handhaving.[4]

Gelet op de accentverschuiving richting toezicht en handhaving is het opvallend dat het CBP in de onderzoeksperiode slechts mondjesmaat sanctie-instrumenten heeft toegepast (in 2005 9 boetes en 2 dwangsommen; in 2006 3 boetes en geen dwangsommen en in 2007 geen boetes en 39 dwangsommen). In 2007 heeft het college besloten geen prioriteit te geven aan onderzoek naar de meldingsplicht, vanwege de verwachting dat organisaties zich redelijk tot goed aan die plicht conformeren. Het college geeft aan over te weinig effectieve handhavingsinstrumenten te beschikken; de bestuurlijke boete zou volgens het college op meer overtredingen van bepalingen van de wet van toepassing moeten worden verklaard. Die wens is opvallend gelet op het toch relatief geringe aantal dwangsombesluiten dat de afgelopen jaren is vastgesteld. Dat roept de vraag op of wellicht effectief toezicht kan worden uitgeoefend door te dreigen met de inzet van handhavingsmiddelen.

Het kostte grote moeite betrokkenen te vinden die hebben geklaagd of die een geschil over toepassing van de wet aanhangig hebben gemaakt. Onbekendheid met de mogelijkheden speelt een rol, evengoed als het ontbreken van intermediairen die hier een verbindende rol kunnen spelen. De op dit vlak gespecialiseerde rechtshulpverleners zijn doorgaans werkzaam bij de grotere kantoren, waardoor de financiële drempel voor een betrokkene aanzienlijk is. Privacybelangen in juridische procedures spelen veelal in de context van een ander geschil, bijvoorbeeld over ontslag of een financiële kwestie. Er doet zich een soort NIMBY-effect voor: privacy in het algemeen wordt door burgers niet zo van belang geacht, maar als in enig conflict de privacy van het individu aan de orde is, is het onderwerp opeens hoogst relevant. Maar al met al is er dus betrekkelijk weinig jurisprudentie over de wet en voor zover die er wel is, is die slecht ontsloten. Bij de Nationale ombudsman worden wel met enige regelmaat klachten aanhangig gemaakt, maar omdat de ombudsman alleen bevoegd is ten aanzien van overheden levert dat geen compleet beeld op.

6. Conclusie

Uit het onderzoek komt als beeld naar voren dat de doelstellingen van de WBP, het waarborgen van evenwicht tussen het privacybelang en andere belangen en het versterken van de positie van personen van wie gegevens worden verwerkt, nog niet ten volle worden gerealiseerd. Uit het enquêteonderzoek, interviews met experts, FG's, vertegenwoordigers van burgerbelangen, casestudies en interviews met burgers die een geschil aanhangig hebben gemaakt, kan worden afgeleid dat de wet in de rechtspraktijk nog niet erg leeft en betrekkelijk lastig hanteerbaar wordt geacht. Duidelijk is dat een op de toepassing gerichte privacygemeenschap en -cultuur nog niet in de volle breedte tot ontwikkeling is gekomen. Het onderzoek ademt een sfeer van rechtssubjecten die zich met enige terughoudendheid in de wet verdiepen.

4 Zie <www.minbzk.nl/116506/advies-over>.

Tegelijkertijd is van belang dat de WBP nog niet erg lang bestaat, hoewel ze in de WPR een verwante rechtsvoorganger had. Kenmerkend voor de WBP is dat het gaat om een wettelijke regeling met open normen die nadere invulling behoeven. Dat kost tijd. En – zo luidt een rode draad van de onderzoeksbevindingen – de rechtsontwikkeling in de zin van sectorale normen en jurisprudentie, die vraagt om contextspecifieke kennis (branche, sector, technologie), is nog niet over de hele linie uitgekristalliseerd.

Dat de wet bestaat uit open normen die in de rechtspraktijk nadere invulling behoeven, is op zichzelf geen knelpunt. Het wordt pas een knelpunt als blijkt dat nadere normering door middel van gedragscodes en regelingen per branche of sector niet tot ontwikkeling komt. Ruim de helft van de organisaties en branches beschikt over een privacycode, maar daar staat dus tegenover dat veel organisaties nog geen nadere regelingen kennen.

Waar een doelstelling van de wet is het toekennen van een inzage- en correctierecht aan betrokkenen, is het van belang op te merken dat uit het onderzoek naar voren komt dat betrokkenen slechts in zeer beperkte mate van die rechten gebruikmaken. De meeste in de enquête betrokken organisaties stellen dat ze betrokkenen via allerlei kanalen informeren over de verwerking van hun persoonsgegevens. Niettemin kan de conclusie dat betrokkenen maar weinig van hun inzage- en correctierechten gebruikmaken, erop wijzen dat zij onvoldoende bekend zijn met de rechten van inzage, correctie en verwijdering. Nader onderzoek zou dat aan het licht kunnen brengen.

Organisaties kunnen – meestal op vrijwillige basis – een FG benoemen. De activiteiten van een dergelijke functionaris lijken in de praktijk bij te dragen aan een bewuste omgang met persoonsgegevens binnen die organisaties. Toch is er bij slechts 0,3 promille van de organisaties in ons land een FG aangesteld. Aanstelling van een dergelijke functionaris zou voor veel organisaties ook een te zwaar middel zijn om privacybescherming te waarborgen. Daarom is het wenselijk dat, meer dan tot op heden praktijk is, organisaties gezamenlijk, branchegewijs, overgaan tot de aanstelling van een FG, zoals artikel 62 WBP mogelijk maakt. Het belang van de functie zou ook verder kunnen toenemen door daaraan meer dan op dit moment eisen te stellen op het vlak van kwaliteit, opleiding en vaardigheden.

De bedoeling van de verplichting om in beginsel alle verwerkingen van persoonsgegevens te melden, is om de bewustwording van de omgang met die gegevens te versterken en de naleving van het doelbindingsprincipe te bevorderen. De praktijk bij de onderzochte organisaties die een melding hebben gedaan, laat inderdaad een zekere terughoudendheid zien bij het gebruik van persoonsgegevens voor andere doelen dan waarvoor zij oorspronkelijk zijn verzameld. Tegelijkertijd lijkt er in veel organisaties ook sprake te zijn van onbekendheid met de normen van de wet. De melding lijkt inderdaad een preventief effect te hebben op het ongebreidelde gebruik van persoonsgegevens binnen de desbetreffende organisaties, maar minder dan 25 procent van de organisaties doet een melding. Opnemen van een melding in het

meldingenregister bij het CBP lijkt op zichzelf niet erg zinvol. Het register lijkt in slechts (zeer) beperkte mate door betrokkenen te worden geraadpleegd.

Over de taakuitoefening door het CBP bestaat wisselende tevredenheid. Aan de ene kant worden de richtsnoeren, adviezen en bemiddelingen door het CBP op prijs gesteld. Aan de andere kant wordt nog meer van het CBP verwacht op het vlak van 'compliance assistance': informatievoorziening en advisering. Er is veel behoefte aan uitleg en interpretatie van de wet, juist waar een op privacybescherming gerichte gemeenschap van vakgenoten of belangenbehartigingsorganisaties nog niet bestaat. Investeringen in de kennisfunctie rond de privacybescherming lijken dringend noodzakelijk. Tegelijkertijd bestaat er breed begrip voor de noodzaak voor het CBP keuzes te maken. En er moet ook worden vastgesteld dat het CBP niet belast is met een wettelijk voorgeschreven adviestaak (behoudens advisering over wetgeving). Hoewel het CBP keuzes moet maken, gelet op de beperkt beschikbare mensen en middelen, is het de vraag of de keuze voor toezicht, tegen de achtergrond van de achterblijvende rechtsontwikkeling, niet te vroeg is gemaakt. Voortgaande investeringen in ontwikkeling en kennisbevordering zouden op (middel)lange termijn mogelijk beter renderen en op den duur een accent op toezicht kunnen rechtvaardigen. Maar er is ook een ander gedachtegang mogelijk, waarin die keuze voor toezicht en handhaving juist leidt tot het ontstaan van initiatieven elders rond voorlichting, bewustwording en normontwikkeling.

Het onderzoek naar de werking van de WBP bevestigt dat het tijd kost voordat wettelijke normen ingang vinden in de praktijk. Juist omdat de wet veel open normen bevat, moet de rechtsontwikkeling in de vorm van nadere normstelling en jurisprudentie ruimte worden gegund. Hoewel in ruim de helft van de organisaties een privacyregeling van kracht is, zijn er (dus) ook veel organisaties die nog steeds een nadere regeling ontberen. De kennis over de wet moet groter worden en de bewustwording bij verantwoordelijken en betrokkenen moet nog groeien. Experts menen dat het belang van privacybescherming zal toenemen als gevolg van technologische ontwikkelingen. Het intensiveren van de toezichtinspanningen kan daarbij een rol spelen, maar ook zouden betrokkenen kunnen worden geactiveerd inspanningen te leveren ten behoeve van het privacybelang. Normontwikkeling, voorlichting en advisering op maat behoeven nadrukkelijk aandacht.